第３次高知県情報セキュリティクラウド構築等委託業務

仕様書（第１.０版）

版数	日付	変更箇所	変更内容
１．０	令和８年　月　日 （契約日）		初版

高知県総合企画部デジタル政策課

第１章　基本事項

１　目的

本業務は、現行の第２次高知県情報セキュリティクラウド（以下「第２次」という。）が令和８年度末に運用期限を迎えることから、令和８年度末までに第３次高知県情報セキュリティクラウド（以下「セキュリティクラウド」又は「第３次」という。）の構築・移行を行い、令和９年度から令和 13 年度までの運用を行うものである。

第３次の目的としては、現行のαモデルを基本としつつも、自治体 DX の進展に伴うβモデルへの円滑な移行、および SaaS 利用の拡大に柔軟に対応可能な拡張性の高いプラットフォームを構築し、セキュリティ水準の確保とコストの抑制を図ることにある。

構築・運用においては、引き続き県が主体となり、令和７年１月 31 日に総務省自治行政局デジタル基盤推進室から示された「自治体情報セキュリティクラウドについて」を踏まえ、国が示す機能要件をベースとして、県が必要とする機能を提供すること。

行政手続のオンライン化、テレワーク環境整備、「α’モデル・βモデル・β’モデル」への将来的なネットワーク構成変更に柔軟に実現できる提案を行うこと。具体的には、SD-WAN 等の技術活用により、トラフィックの増大や経路変更に迅速に対応可能な構成とするなどが想定される。

また、次々期では、GSS、ゼロトラストアーキテクチャを見据えた技術情報を提供するとともに、国の動向に合わせて柔軟に対応が可能な構成とすること。基盤となる ID 管理やログの統合管理について、将来的な連携可能性を考慮した設計とすることなどが想定される。

なお、本仕様書で用いる用語・略語の定義を別紙１に示す。

２　業務の概要

（１）セキュリティクラウドの設計・構築

（２）セキュリティクラウドの利用に必要となるネットワークの敷設・設定

（３）移行設計・移行支援

（４）セキュリティクラウドの運用保守

３　システムの構成

セキュリティクラウドは、図１のとおり、インターネット接続系セグメント、LGWAN 接続系セグメント、共同利用セグメント、ゲートウェイセグメント、運用監視／管理セグメントから構成される。

セキュリティクラウドに接続・利用する団体（以下「接続団体」という。）のインターネット接続系セグメント及び LGWAN 接続系セグメントからは、それぞれアクセス回線として、セキュリティクラウドインターネット VPN、市町村 VPN 等によって接続される。

（１）インターネット接続系セグメント

インターネット接続系に係るサーバを配置するセグメントを意味する。また、DMZ は当セグメントに包括される整理とする。

（２）LGWAN 接続系セグメント

LGWAN 接続系に係るサーバを配置するセグメントを意味する。また、共同利用セグメントは当セグメントに包括される整理とする。

（３）共同利用セグメント

複数の接続団体が共同で利用するアプリケーション及びセキュリティクラウドポータルサイトを配置するセグメントを意味する。

（4）ゲートウェイセグメント

インターネット接続系セグメントと LGWAN 接続系セグメントとの中継に係るセグメントを意味する当セグメントにおいて、インターネット接続系と LGWAN 接続系間の分離を行う。

（5）運用監視／管理セグメント

運用監視／管理に係るサーバ及びリモートメンテナンス専用ファイアウォールを配置するセグメントを意味する。

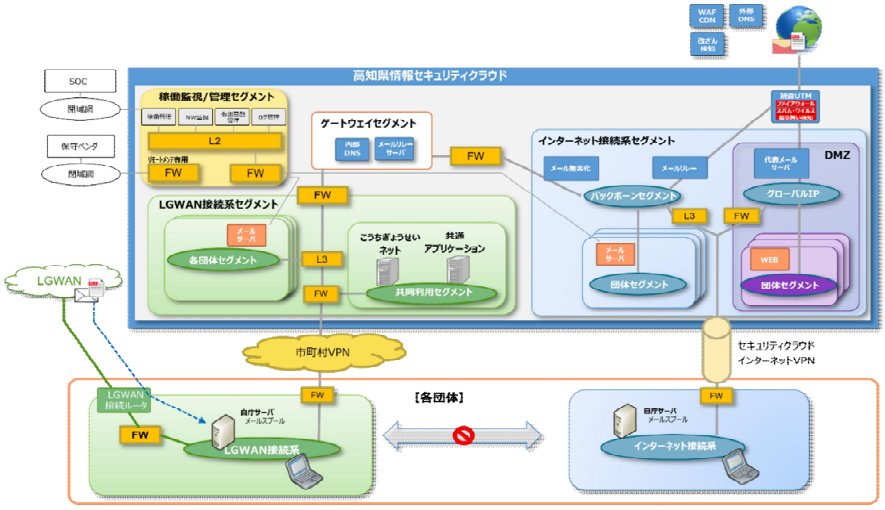

図１　セキュリティクラウド概要図

4　業務の範囲

本業務の範囲を以下に示す。各作業の進め方については、プロジェクト計画立案の段階で県と調整し、承認を得ること。なお、（1）～（6）については令和８年度中に実施し、（7）は令和９年度～令和 13 年度に実施する。

（1）全体プロジェクト管理

プロジェクト計画を立案し、体制図・要員配置、進捗管理、品質管理、リスク管理など、本業務に関わる各種事項について総合的な管理を行う。

（2）要件定義

機能、性能、ネットワーク、運用に係る要件定義を行う。

（3）設計及びテスト計画

①機能設計

機能要件及び性能要件に基づき、機能設計及びテスト計画作成を行う。

②ネットワーク設計

機能要件、性能要件及び各接続団体の要件に基づき、ネットワークの設計を行う。

③運用設計

稼働後の運用及び障害対応、セキュリティ監視やセキュリティインシデント対応等についての設計及びテスト計画作成を行う。

（4）設定

①環境設定

各種設計に基づき、必要資源の設置及び設定を行う。

②ネットワーク設定

ネットワーク設計に基づき、必要資源の設置及び設定を行う。

（5）テスト

①機能テスト

テスト計画に基づき、各接続団体のセキュリティクラウドへの接続及び必要機能の動作を検証する。

②運用テスト

日次・月次・年次のサイクルテスト及び性能・信頼性等の非機能要件を満たしていることを検証する。

（6）移行切替(第２次からの移行切替に係る作業一式)

①計画作成

第２次から移行が必要な資産・環境を調査し、全体及び個別資産の移行計画・移行手順を作成する。

②テスト及び実施

移行切替リハーサル及び移行切替を実施する。

③接続団体移行切替

各接続団体へのヒアリングに基づき、団体ごとの移行計画・移行手順(役割分担)を作成し、各団体の移行切替作業を役割分担に応じて実施する。

（7）セキュリティクラウドの運用保守等

①セキュリティ対応業務

情報セキュリティの監視(SOC 監視体制※)及びセキュリティインシデントへの対応を実施する。

※24 時間 365 日(閏年は 366 日)セキュリティ機器を監視しサイバー攻撃の検出や分析、対策などのアドバイスを行う組織

②運用保守業務

ヘルプデスク業務、運用サポート業務、定期報告(月次・年次)を実施する。

③受託事業者における責任範囲

図２のとおり、セキュリティクラウドに接続する高知県情報ハイウェイ(以下「情報ハイウェイ」という。)におけるセキュリティクラウド拠点内回線収容装置のセキュリティクラウド側インターフェイスを責任分界点とする。ただし、接続団体に設置されたセキュリティクラウド接続ルータについては、セキュリティクラウドの責任範囲とするが、接続団体も当該ルータに係る善管注意義務を負うものとする。

セキュリティクラウドへのアクセス回線は、接続団体が設置及び保守するものとするが、アクセス回線として情報ハイウェイを利用する場合は、情報ハイウェイの概要は第２章２（２）②を参照すること。接続団体の直近のアクセスポイント内回線収容装置の接続団体側インターフェイスから接続団体側を、接続団体の責任範囲とする。

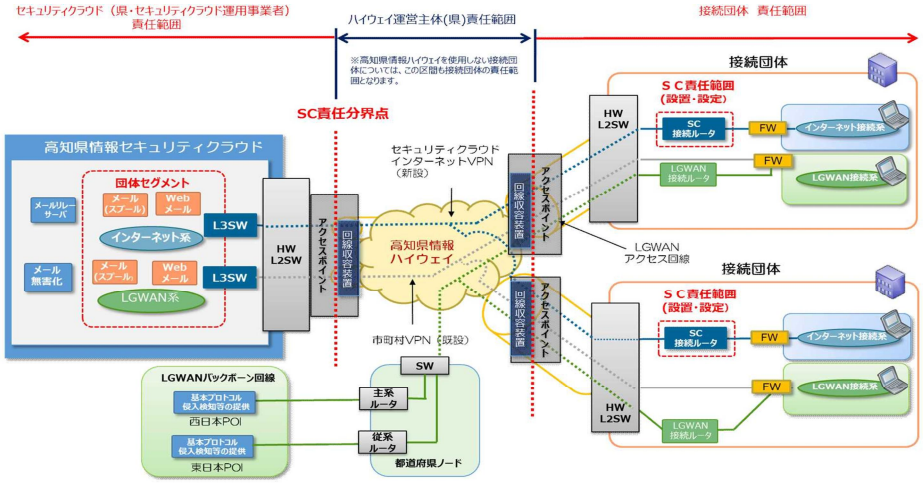

図２　セキュリティクラウドにおける責任分界点

④セキュリティインシデント発生時における責任範囲

SOC によるセキュリティインシデントの検知、影響範囲、攻撃内容の分析を元に、セキュリティクラウド側でセキュリティ機器、ネットワーク機器のオペレーションを行う。併せて、県及び発生元となる接続団体への通知及び対策支援を行うことをセキュリティクラウドの責任範囲とする。

なお、接続団体内における端末の特定、証拠証跡の確保及び接続団体内における対策の実施は、接続団体の責任範囲とする。

（８）第４次高知県情報セキュリティクラウドへの移行支援

本業務終了後、第４次高知県情報セキュリティクラウド（以下「第４次」という。）への円滑な移行を行うために必要な情報提供及び支援作業を実施するために、次のことを行うこととする。

①技術情報の提供

次々期システムの要件定義および設計に必要な現行システムの論理構成図、パラメータシート、ポリシー設定一覧、および資産管理情報等の最新版を提供すること。

②移行データの作成

蓄積されたセキュリティログ、統計データ、各接続団体の個別設定情報等を、次々期ベンダーが活用可能な標準的データ形式（CSV，JSON 等）で整理・抽出すること。

③ナレッジ移管

過去の障害対応履歴、運用上の特記事項、各団体特有の留意事項について、引継書を作成し、次々期事業者への説明会を実施すること。

④並行運用および切替支援

新旧システムの並行稼働期間中、安全な切替えに向けた経路制御の変更協力や、トラブル発生時の切り戻し対応に協力すること。

各作業の役割分担を表１に示す。

表１　役割分担

項番	作業名称	◎：作業主体 ○：管理 △：支援		
		受託事業者	県	接続団体
1	全体プロジェクト管理	◎	○	
2	要件定義	◎	○	△
3	設計及びテスト計画	◎	○	△
4	設定	◎	○	
5	テスト	◎	○	△
6	移行切替	◎	○	△
7	セキュリティクラウドの運用保守等	◎	○	
8	第４次への移行支援	◎	○	△

５　納入成果物

（１）納入成果物及び期限

受託者は、別紙２に示す納入成果物を作成し、県が指定する場所に期日までに提出し、県の承認を得ること。

（２）納入形態

納入成果物は、DVD-R に格納した電子データと、紙面に印刷したもの１部をセットにして納入すること。

電子データは Adobe Reader で閲覧可能な形式とすること。ただし、将来的に更新が必要となる成果物に関しては、Microsoft Office(Word・Excel 等)形式とすること。

（３）納入後の更新について

本業務に係る契約期間中、既に納入済みの成果物に変更が発生した場合には、都度更新版を提出し、県の承認を得ること。更新版の提出に際しては、必ず更新履歴を添付すること。

６　スケジュール

（１）構築・移行：本業務の契約締結日～令和９年３月 31 日
（令和９年２月までには機能検証が終了していること）

（２）運用保守：令和９年４月１日～令和 14 年３月 31 日

（３）第４次への移行：第４次の契約締結日～令和 14 年３月 31 日

７　留意事項

（１）本業務について、契約書及び仕様書に明示されていない事項であっても、その履行上当然必要な事項については、受託事業者が責任を持って対応すること。

（２）本業務に要する経費のうち、令和８年度分はシステムの構築および移行に要する初期経費とし、運用保守費用については、運用開始後の令和９年度以降に分割して発生するよう計画すること。

（３）運用期間中における各接続団体のネットワーク構成変更、クラウドサービス利用の拡大等に伴うリソース増減や設定変更に対し、迅速かつ柔軟に対応可能な構成及び価格体系を提示すること。

（4）受託事業者は以下URLに示す「自治体情報セキュリティクラウド機能要件一覧」に示されている必須要件を満たすサービスを提供すること。

（URL https://www.soumu.go.jp/main_content/000702974.pdf）

（5）サプライチェーン・リスクの管理をはじめとして、「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和７年３月版）」に準拠した情報セキュリティ対策を実施の上、事業を行うこと。

（6）自治体情報セキュリティクラウドを構成するハードウェアやソフトウェアについては事業者所有のサービスを活用する形で更新事業を行うこと。

（7）都道府県の負担する更新費用の算出にあたっては、ハードウェアやソフトウェアを購入する経費を含めないこと。

第２章 システムの要件

１　機能要件

（１）インターネット通信の監視

ア　監視(障害切り分け、通報、セキュリティインシデント管理)

①Web サーバ

・Web サーバへの攻撃・脆弱性等を監視すること。
・ログ分析を行うためアクセス情報(アクセス日時、接続元 IP 等)を記録すること。
・受託事業者がログを分析し、セキュリティインシデントが発生した場合に報告すること。
・接続団体が所有する Web サーバを集約すること。
・オリジナルの Web サーバをリバースプロキシ経由とし、そのリバースプロキシを監視対象としてもよい。
・セキュリティクラウド環境以外（自庁設置又はクラウドサービスに設置されている Web サーバ）を利用する Web サーバも監視対象とすること。
・CDN を利用する場合は、オリジナルサーバのみを監視対象とすること。
・リバースプロキシで集約する場合は、送信元 IP アドレス情報(X-Forwarded-For)を設定し、送信元 IP アドレスを確認できること。

②メールリレーサーバ

・接続団体とインターネットのメールを中継するメールリレーサーバを設置し、通信内容を監視すること。
・ログ分析を行うためアクセス情報(アクセス日時、接続元 IP 等)を記録すること。
・受託事業者がログを分析し、セキュリティインシデントが発生した場合に報告すること。
・不正中継を防止すること。
・なりすましメールに対する対策を講じること。
・SMTP(RFC2821、RFC2822 準拠)を使用した、インターネット経由の電子メールの送受信機能を提供すること。
・中継を許可するドメインは、接続団体が管理するドメインのみとすること。
・送信及び受信ドメイン認証方式として、普及率が最も高い SPF 方式を基本として、これに加えて DKIM 方式、DMARC 方式を併用することでなりすましメールに対する対策ができるようにすること。
・接続団体ごとのマルチドメインをサポートすること。
・外部クラウドサービスを利用する場合は同等の機能を有すること。

③プロキシサーバ

・接続団体の各端末の代理でインターネット閲覧を行い、その通信内容を監視すること。
・ログ分析を行うためアクセス情報(アクセス日時、接続元 IP 等)を記録すること。
・蓄積しているプロキシログを活用して過去の被害状況を調査すること。
・不正通信を行っている端末を特定するため、接続団体が特定できること。
・受託事業者がプロキシログを分析して、不正通信を行っている接続団体を特定する情報の収集を行うこと。
・セキュリティを考慮し、セキュリティクラウドからインターネットへ通信を行う際は、接続団体が管理するプライベートアドレスを秘匿できること。
・複数の端末から同じ大容量ファイルの送受信を行う場合等(ウイルスパターン更新や修正パッチのダウンロード等)を考慮し、セキュリティクラウドの通信負荷を軽減させる提案を行うこと。

④DNS サーバ(外部及び内部)

・接続団体のドメイン情報(サーバのホスト名(URL)とグローバル IP アドレスの変換)をインターネットに公開し、通信内容を監視すること。
・接続団体のキャッシュ DNS サーバとしてインターネットに対して再帰問い合わせを行い、通信内容を監視すること。
・ログ分析を行うためアクセス情報(アクセス日時、接続元 IP 等)を記録すること。
・C&C サーバ等への DNS 問い合わせなど不正な通信を監視し、検知すること。
・受託事業者がログを分析し、セキュリティインシデントが発生した場合に報告すること。
・セキュリティクラウド内部の名前解決及び外部へのフォワードに関するデータを登録し、通信内容を監視すること。
・DNS プロトコル(RFC1034、RFC1035 準拠)を使用した DNS 機能を提供すること。
・インターネット及び各接続団体の端末等から DNS 問い合わせに関する通信ログを最低１年間は記録すること。
・逆引きの名前解決による送信ドメイン認証を行っているメールサーバからのメール受信を可能とするため、逆引きの名前解決を行うこと。
・ゾーン転送は許可されたサーバに対してのみ行うこと。
・IPv6 に対応できること。
・送信ドメイン認証方式として普及率が最も高い SPF 情報を TXT レコードとして提供できること。
・接続団体ごとのマルチドメインをサポートすること。

（２）セキュリティインシデントの予防

ア　ゲートウェイ対策

①ファイアウォール

・IP アドレスやポート番号について、許可及び拒否のルールを設定し、通信を制御すること。また、アプリケーション識別による制御をすること。前段に配置されるプロキシサーバと組み合わせて、IP アドレスの代わりにドメイン名又は FQDN による通信先特定でもよい。
・管理する接続団体ごとに独立した通信を可能とし、相互に干渉することのないよう、適切な通信制御を行うこと。
・利用帯域、接続数に応じた処理性能を有すること。
・インターネットと内部ネットワークをファイアウォールで分離すること。
・通信許可／拒絶のルールは接続団体で共通のルール及び、接続団体で個別のルールを定義できること。
・令和９年度から５年間の通信量増加を踏まえた拡張性を確保すること。
・許可ルールについては、IP アドレスやポート番号の他、限定可能な範囲について明らかにすること。

②IDS/IPS

・インターネットとの通信においてパケットを監視し、シグネチャや異常検出により不正通信を検知及び遮断すること。
・ワーム、トロイの木馬、ウイルス、DDoS 攻撃等の脅威から、サーバ、端末及びネットワーク機器を防御すること。
・シグネチャの更新時に継続してセンサーが稼動し、非監視時間が発生しないこと。
(基本的に、リブートやサービスの再起動が行われないこと)
・管理する接続団体ごとの詳細な設定は実施せず、全団体共通の設定を行うこと。

・シグネチャの更新は、セキュリティベンダーがシグネチャを公開してから、速やかに受託事業者が更新すること。
・通信量を増大させるなどして回線やサーバ機能を占有する DoS/DDoS 攻撃を検知し、遮断すること。
・特定のしきい値を超えてアイドル状態が続いている接続を削除すること。

③マルウェア対策
・Web 通信を監視し、ベンダーが提供するパターンファイルに基づき、マルウェア等の不正プログラムの検知及び遮断を行うこと。
・メール通信を監視し、ベンダーが提供するパターンファイルに基づき、マルウェア等の不正プログラムの検知及び遮断処理を行うこと。
・パターンファイルは、自動更新により常に最新のものを保持すること。
・閲覧するページ内の HTML、画像、ファイルについて、ウイルススキャンを行うこと。
・メールの本文(HTML メール)、画像、添付ファイルについて、ウイルススキャンを行うこと。
・受託事業者がマルウェアを検知した場合、受信者等のメールアドレスへ通知すること。
・インバウンド方向及びアウトバウンド方向のメールを検査すること。
・C&C サーバへの不正な通信を検査すること。

④通信の復号対応
・SSL/TLS で暗号化された通信内容を復号し、通信内容を監視可能とすること。
・通信の復号処理により業務に支障が出る場合は迂回等対応すること。
・通信先が信頼できると判断される場合は、復号処理の対象外とする。
・復号した通信は再度暗号化すること
・通信の復号を行うため、接続する端末に中間証明書を提供すること。

⑤URL フィルタ
・受託事業者がブラックリスト方式及びホワイトリスト方式に対応すること。
・ブラックリストにより不正な IP アドレス及び URL への接続を検知及び遮断すること。
・全接続団体が共通して接続を制限するべき URL 等の設定ができ、かつ、管理する接続団体ごとに設定も可能であること。また、管理する接続団体が定義したリストによるアクセス制限が可能なこと。
・カテゴリごとにアクセス制限可能なこと。
・規制カテゴリは自動メンテナンスされ、新サイトにも自動的に対応すること。
・受託事業者が特定の Web サイト(掲示板等)に対して、書き込み制限できること。
・受託事業者が C&C サーバや悪意のある Web サイトへのアクセスを検知及び遮断すること。
・Web サイトがブロックされた際に、アクセスしたユーザーへ警告画面を表示すること。
・受託事業者が運用にて接続団体の URL フィルタリングルール変更のメンテナンスを行うこと。
・受託事業者が業務との関連性が低い Web ページへの接続を制限すること。

イ　メールセキュリティ対策

①アンチウイルス／スパム対策(インターネット系)
・インターネットからのメールについて、アンチウイルス検査を行い、不正なメールの検知、隔離及び削除を行うこと。
・インターネットからのメールについて、スパムメールの判別を行い、レベルに応じた隔離及び遮断を行うこと。
・受託事業者が業務に不要な広告メール等を検知し隔離及び遮断できること。
・受託事業者がブラックリスト方式、ホワイトリスト方式に対応すること。
・メール原本は隔離されたサーバに転送できること。

・セキュリティクラウド共通の迷惑メールフィルタリングを設定すること。
・隔離されたメールは一定期間保存され、必要に応じて確認ができること。

②振る舞い検知機能
・インターネットからのファイル等を仮想環境で動作させて挙動を監視し、未知のマルウェア等の不正プログラムを検知可能な機能を有すること。
・コールバックする通信について、検知及び停止すること。
・メールの本文に記載される URL リンクを仮想環境にて検査すること。
・外部と多大な通信をすることなくマルウェアを解析すること。
(本来のインターネットトラフィックにインパクトを与えない)
・マルウェアを検出した場合は、県が指定した宛先へ通知すること。また、判定結果が脅威であった通信については、その通信を遮断すること。
・インバウンド方向のみを対象として振る舞い検知を行い、アウトバウンド方向については振る舞い検知を行わないこと。ただし、アウトバウンド方向の監視についても柔軟に対応可能な構成とすること。
・ZIP 等の圧縮形式の添付ファイルについても検査を行うこと。

ウ　メール及びインターネットセキュリティ対策
①メール無害化
・メールの添付ファイルは削除し、LGWAN 系へ転送できること。
・HTML メールをテキスト化して転送できること。
・メール原本は隔離されたサーバに転送できること。
・無害化処理したメールに対して、タイトルに無害化処理をしたことを容易に判断可能であること。
・添付ファイルの拡張子やメール本文などを条件に、メールの受信拒否、メール本文への注意喚起の挿入、接続団体の管理者への通知などのアクションを実施でき、拡張子は RLO の偽装が実施されている場合においても正しい拡張子で判定できる機能を有すること。
②ファイル無害化
・インターネットから受信されるファイルを検査し、ファイルを削除、マルウェア検査、サニタイズ処理などの機能を持ち、無害化を行ったファイルを LGWAN 接続系に転送できること。
・LGWAN 系からインターネット系へのファイル無害化にも対応すること。
・ファイルのヘッダーや OLE オブジェクトなどから当該ファイルのフォーマットを認識し、ファイル構造に当てはまらなかったコンテンツを削除すること及びマクロ等マルウェアが存在する可能性を強制的に削除することでファイルを無害化し、マルウェアに感染するリスクを低減させること。
・ファイルを開かずに無害化処理を実施すること。
・無害化ファイルの取り出し時、第三者承認を要求できる機能を有すること。
・無害化の履歴(ログ)を記録し、接続団体の管理者が確認できること。(利用者 ID、ファイル名、無害化日時、承認者 ID、承認日時等)
・県の指示を受け、受託事業者がシステム全体の設定に加えて、任意のグループに対する設定が行えること。
・Microsoft Office ファイルのマクロ、OLE、ハイパーリンク、ActiveX、DDE の除去、PDF ファイルのスクリプト、ハイパーリンク、オープンアクション、添付ファイル、埋め込みフォントの除去、HTML ファイルに含まれる JavaScript および外部リソースへのリンクの無効化、CSV ファイルに含まれる数式（=から始まる文字列）の無効化、圧縮ファイルを展開し内部のファイルを再帰的に無害化すること。

・ユーザー数は構成団体の全職員が利用可能であること。
・無害化対象ファイルはMicrosoft Officeの各ファイル、PDF、画像ファイル、圧縮ファイル、一太郎ファイル、CADファイル、DocuWorks、HTMLファイル、CSVファイル等を想定する。

③Web振る舞い検知
・インターネットとの通信で受信するファイルについて、隔離した疑似環境で動作させ、マルウェアのような異常な動作をするプログラムやリスクの高いファイル等を検知する機能を提供すること。
・Webサイトからダウンロードしたファイルも同様に振る舞い検知にかけ、不正なプログラム等が検知された場合はダウンロードさせないこと。
・擬似環境となるサンドボックスは、インターネット上に機能を持つか、もしくは専用の装置を設置すること。

エ　Webサーバセキュリティ対策

①WAF
・接続団体が管理するWebサイトに対して、Webアプリケーションの脆弱性を狙った不正な通信等を検知・防御すること。
・受託事業者が管理する接続団体のWebサーバに合わせて必要なチューニング等を行うこと。
・SSL通信については、受託事業者が各Webサーバのサーバ証明書と鍵を保有してSSL通信を復号化し、必要なセキュリティ検査を行うこと。
・Webアプリケーションの脆弱性を突いた以下の攻撃を防御すること。
SQLインジェクション／OSコマンド・インジェクション／ディレクトリ・トラバーサル／セッション管理の不備／クロスサイト・スクリプティング／CSRF(クロスサイト・リクエスト・フォージェリ)／HTTPヘッダ・インジェクション／メールヘッダ・インジェクション／クリックジャッキング／バッファオーバーフロー／アクセス制御や認可制御の欠落
・バックドアの検疫、無害化機能を標準機能として有していること。

②CDN
・大規模なリクエストが発生した場合でも継続的な情報発信ができるようWebサーバの負荷分散を行うこと。
・接続団体のWebサイト(Webサーバ)に急激なアクセスがあった場合においても、住民に対してWebサイトから情報が継続的に発信可能なサービスであること。
・CDNを利用するWebサーバは接続団体の公式Webサーバ及びアクセス集中が想定されるサーバを対象とすること。
・コンテンツキャッシュサーバは、インターネット上の複数のサーバで構成され高速な配信を実現すること。
・CDNサービスが提供されるサービスは、耐震、免震などの構造上の安全性に配慮された設備で運用された可用性が高いサービスであること。
・HTTPSでコンテンツを配信可能であること。
・HTTPSの場合はサーバ証明書も提供できること。
・アクセス元のIPアドレスに応じたアクセス拒否／許可の設定が可能であること。
・アクセスログを取得可能であること。
・接続団体のWebサイトを運用するサーバの設置場所に応じてCDNサービスが提供可能なこと。
Ａ）セキュリティクラウド内でオリジンサーバ(接続団体のWebサイトを運用しているサーバ)を集約しているケース

Ｂ）市町村等の環境（オンプレミス・クラウドサービス）でオリジンサーバを運営しているケース

・年度単位で定額でのサービス提供が可能であること。
・Web サイトへのアクセス数が急増した場合もサービスが停止しないこと。
・転送量の状況などサポートポータルで確認できること。
・DDoS 対策機能、WAF 機能がオプションサービスとして用意されていること。
・IPv6 でコンテンツ配信可能であること。
・HTTP、HTTPS にキャッシュルールを設定可能であること。
・CDN でキャッシュを有効とするコンテンツはコンテンツ制作者と協議し、登録すること。

③コンテンツ改ざん検知

・接続団体の Web サーバ上のコンテンツが第三者によって不正に書き換えられた場合、検知する機能を有すること。
・既存の Web サーバの改修が必要にならないエージェントレス型の改ざん検知機能を提供すること。
・外部サービスを利用して公開している場合もコンテンツ改ざんの検知を行うこと。
・コンテンツ内容の改ざんを検知し通知すること、アラートはメール等で接続団体の管理者に通知できること。
・受託事業者が Web サーバアプリケーション(IIS、Apache 等)に限定されず改ざんを検知できること。
・県参考値：85URL、総ページ数：20 万ページ。
・改ざん検知時に、閲覧者を安全なページへ自動的に警告画面へ遷移すること。
・コンテンツ内に含まれる外部 JavaScript ファイル、CSS の改ざんの検査が行えること。
・リンク先のマルウェア検知ができること。

（３）SOC 運用サービス

①ログ収集・分析

・ファイアウォール、IDS/IPS といったセキュリティ機器や監視対象サーバ(Web サーバ、メールリレーサーバ、プロキシサーバ、外部 DNS サーバ)が出力したログを収集し、不正な現象を検知すること。
・ファイアウォールのログについて、拒否(deny)だけでなく、許可(Allow)ルールが適用された際のログを収集・分析すること。
・ログは最低５年分保存できること。
・ログの時刻は NTP による時刻同期が常に行われ、正確に管理されていること。
・自治体からの要求に応じて、過去のログを迅速に検索・抽出し、速やかに提供できる体制を有していること。
・必要なルールを個別に作成できること。
・ログ収集の対象となる機器との間に動作実績があること。
・収集されたデータを効率的に保存及び圧縮できること。
・要求する運用に対応可能な機器、機能を提供できること。
・セキュリティ機器が出力したログからセキュリティインシデントの兆候が見られた場合は、受託事業者が監視対象サーバ(Web サーバ、メールリレーサーバ、プロキシサーバ、外部 DNS サーバ)や、ゲートウェイ対策システム(マルウェア検知、プロキシサーバ、URL フィルタ)、メールセキュリティ対策システム(アンチウイルス／スパム対策、振る舞い検知機能、メール無害化／ファイル無害化)が出力したログの調査を実施し、迅速な対応を行うこと。
・受託事業者が複数の機器のログから関連するログを抽出して、相関関係の分析を行い、セキュリティインシデントの兆候をつかむことで迅速な対応をすること。

②イベント監視

・受託事業者がファイアウォール、IDS/IPS といったセキュリティ機器や監視対象サーバ(Web サーバ、メールリレーサーバ、プロキシサーバ、外部 DNS サーバ)のイベントを監視し、異常を検知した際に通知できること。
・パターンマッチングやしきい値等のルールに基づき、許可していないイベントの発生を検知できること。
・OS のシステムイベント、アプリ―ションの起動や停止、エラー通知といったイベントを監視できること。
・受託事業者が検知したイベントはログとして保存すること。
・セキュリティインシデントの兆候をつかむために有用でないイベントは除外(フィルタリング)できること。

③マネージドセキュリティサービス
・高度な人材(セキュリティ専門家)によるログ監視、分析によりセキュリティインシデントの発生を予防すること。
・以下の事項について有人で 24 時間 365 日(閏年は 366 日)対応できること。
Ａ）アナリストによるログ分析及びログ監視
Ｂ）セキュリティインシデントの発生又はそれが疑われる場合に、接続団体への通知及び原因の速やかな特定
Ｃ）セキュリティインシデント発生時に、監視対象システムに対して直接又はシステムの保守担当者と連携して ACL 追加など、被害拡大防止のための技術的な一次対応
・脅威情報を用い、監視対象システムの環境に応じた重大度の判定及び接続団体への通知ができること。
・監視対象システムが発報するアラートをそのまま通知するのではなく、分析を行い、誤検知を排除した上で接続団体へ通知すること。
・セキュリティインシデント発生後、接続団体へ通知するまでの時間などの SLA については事前に提示すること。
・監視対象システムの設定に不備が見られる場合、接続団体に連絡・確認し、必要に応じて接続団体にシステムへの対応について指示できること。
・接続団体の CSIRT 又は接続団体の CSIRT を直接サポート(ヘルプデスクに相当)する事業者に対して、障害・セキュリティインシデントに対する助言や問い合わせの対応を行うこと。
・適切な監視の維持のために、監視対象システムの環境にある監視用の機器又はソフトウェアのメンテナンスを実施すること。また、監視対象システムに対して以下の事項が行えること。
Ａ）死活監視及び異常発生時の接続団体への通知
Ｂ）リソース監視及び異常発生時の接続団体への通知
・セキュリティインシデント発生時に ACL 追加などの一次対応を迅速に行うため、監視対象システムの運用管理を行う部門との迅速な連携ができる体制を整えること。
・経済産業省の情報セキュリティサービス審査登録制度の情報セキュリティサービス基準を満たす事業者を選定すること。(技術要件、品質管理要件を共に満たすこと)
・セキュリティ機器や監視対象サーバ(Web サーバ、メールリレーサーバ、プロキシサーバ、外部 DNS サーバ)のログ監視方法について、次のいずれかの方法で行うこと。
Ａ)監視対象のログをすべてマネージドセキュリティサービス事業者側に送り、監視する方法
Ｂ)監視対象のログの一部をマネージドセキュリティサービス事業者側に送り、必要に応じて、マネージドセキュリティサービス事業者がログ収集のために設置しているセキュリティ機器にマネージドセキュリティサービスが遠隔からアクセスし、保存されているログを閲覧、監視する方法

（４）対応と復旧

①システム・サービス構成管理

・セキュリティクラウドを安定的に稼働させるため、構成する各機器、ソフトウェア、サービスのバージョン情報、ベンダー情報などを管理すること。
・構成する各機器、ソフトウェア、サービスについて以下を実施すること。
　Ａ）シグネチャが定期的にアップデートされていることを確認すること
　Ｂ）許可、拒否ルールを管理し、定期的に見直しを行うこと
　Ｃ）サポート期間が超過していないことを確認すること

②脆弱性情報の入手と該当製品への対応及びセキュリティレベルの自己点検

・安全なシステム運用を実現するため、構成する機器、ソフトウェアの脆弱性情報を収集し、適宜ファームウェアアップデート／不具合修正パッチ適用／セキュリティパッチ適用を実施すること。パッチ適用に際しては、事前に本番環境への影響を評価し、県の承認を得た上で実施すること。
・セキュリティレベルの自己点検として、年１回、構成する機器に対しての脆弱性診断を実施して脆弱性がないか検証すること。脆弱性が検知された場合、速やかに是正すること。
・受託事業者が必要に応じて機器、ソフトウェアのバージョンアップを行うこと。
・システム停止等が困難な場合、設定変更等による脆弱性の回避策についても受託事業者が検討し、提言すること。
・脆弱性情報は受託事業者が JPCERT など公開情報を適宜参照すること。

③不正通信の早期検知を行う運用体制の確立(CSIRT)

・セキュリティインシデント発生時の対応を迅速に行うため運用体制(CSIRT)を構築すること。
・運用体制を書面にて県に共有すること。
・運用フローを年１回以上検証すること。
・ポータルサイトによる情報共有を行うこと。
・セキュリティインシデント発生時、必要に応じてファイアウォールのポリシー追加、変更により通信を遮断すること。ポリシー変更は県と協議のうえ、決定すること。また、事前決定された対応案に基づいて実施すること。
・接続団体及び県を含め、セキュリティインシデントの発生を想定した訓練を受託事業者が年１回以上行うこと。

④障害管理(問題管理、変更管理、復旧対応)

・セキュリティクラウドを構成する機器は冗長化を行い、単一障害時での業務継続を可能とすること。
・セキュリティクラウドを構成する機器の監視を行い、受託事業者が障害発生時速やかに復旧を行うこと。
・受託事業者がセキュリティクラウドを構成する機器の稼働ログ、エラーログを収集し、障害発生原因を分析できるようにすること。また、ログ分析により障害予防に努めること。
・取得対象ログはネットワークスイッチ、ルータ、管理系サーバ等セキュリティクラウドを構成する機器全般を対象とすること。
・構成する機器、ソフトウェア等に関してベンダー保守を締結すること。
・障害管理を適切に行い定例会議等において関係者間で共有すること。

⑤バックアップとリストア

・システム障害やサイバー攻撃によるデータ消失やマルウェア被害等の対策として、バックアップを取得し、迅速なリカバリ対応をできるように対策を講じることで、業務継続性を担保すること。
・機器障害などによりセキュリティクラウドの運用が停止することを防ぐため、バックアップを取得すること。
・ログ等日々の保存データを日次でバックアップすること。
・システム変更が生じた場合、随時システムバックアップを行うこと。
・バックアップからのリストアを運用開始前に検証すること。
・バックアップはオリジナルデータとは別の場所に保管し、本体障害時に復旧できること。
・機器及びサーバの復旧が必要な場合は、受託事業者がシステム又は設定のリストアを行うこと。

（５）県固有要件

ア　オンラインストレージ

①大容量ファイル転送

・インターネット系ネットワーク及びLGWAN系ネットワークで利用できるファイルストレージ機能を提供すること。
・LGWAN系ネットワークで利用できるファイルストレージを通知する際には、通知文書が無害化されないこと。あわせて、LGWAN系とインターネット系と区別した通知文書とすること。
・メールに添付できない大容量(一度に送信できるファイルサイズ１GB)のファイルを取扱いできること。(ディスク容量は500GB以上)
・セキュリティクラウド内外の送受信ファイルのウイルスチェック及び圧縮・暗号化やSSL通信によるセキュリティ対策等により安全に送信できること。
・ファイルについては、１週間保持でき、登録後１週間を超えたファイルについては自動削除されること。
・アクセスIP制限(庁内であればローカルIPで制限、外部からはグローバルIPで制限)が可能なこと。
・ユーザー数は構成団体の全職員が使用できることを想定すること。

イ　共同利用セグメント

①共同利用セグメント資産の移行

・共同利用セグメントには、複数の接続団体が共同で利用するアプリケーション及びセキュリティクラウドポータルサイトが配置されており、これらを第３次でも継続して利用できるよう移行を行う。共同利用セグメントの資産については、別紙３に記載。
・アプリケーションを搭載するための仮想基盤及びその上で稼働する仮想マシンを提供すること。
・第２次の共同利用セグメントで稼働している仮想サーバを移行し、第３次の共同利用セグメントでの正常稼働を保証すること。
・第２次の共同利用セグメントは第３次内のハウジングスペースで物理サーバのハウジングを行っており、第３次の共同利用セグメントにおいても同様のハウジングサービスを提供し、正常稼働を保証すること。

②共同利用セグメント接続環境の移行

・第２次の共同利用セグメントと接続している外部データセンターについて、第３次の共同利用セグメントにおいて接続を継承し、第２次と同様のアクセス環境を提供すること。また、このための回線替え等の方法及び費用について提案すること。

・第２次の共同利用セグメントはアクセス回線として情報ハイウェイ内の市町村 VPN を使用している。第３次の共同利用セグメントにおいても同様のアクセス環境を提供すること。また、このために接続団体側で設定変更が必要な場合は、具体的な作業内容と概算費用について提案すること。
・第２次の共同利用セグメントでは DNS による名前解決を行っており、第３次の共同利用セグメントにおいてもこの機能を継承すること。
・共同利用セグメントを利用しているサーバに対して死活監視を行うこと。

③共同利用セグメントのドメイン
・共同利用セグメントで利用するドメイン名については、既存のものを使用すること。

ウ　ポータルサイト

①ポータルサイトの構築・運用
・セキュリティクラウド内共同利用セグメントにおいて、接続団体向けに掲示板機能(「こうちぎょうせいネット」を含む)を提供すること。ポータルサイトの機能概要は、別紙４を参照。
・ポータルサイトは、セキュリティクラウドの運用状況、セキュリティインシデントの発生状況及び対策状況、各種レポート類などの有用な情報を迅速に接続団体に情報提供できること。
・ポータルサイトにセキュリティクラウド運用に関する各種手順書、ガイドライン、各種様式等ドキュメントを掲載し、接続団体から閲覧及びダウンロードできる状態にすること。
・第２次の掲載記事やアップロードファイルが第３次でも参照及び更新できるよう移行すること。
・ポータルサイトの電子メールや入力フォーム等の機能により、接続団体からのユーザー状況のメンテナンス依頼が行えること。
・ポータルサイトにアクセスする接続団体ごとにアカウントを発行し、認証を行うこと。
・ポータルサイトは接続団体の LGWAN 系セグメントからアクセスできる構成とすること。
・第２次の改善点について県と協議のうえ、対応を行うこと。

②こうちぎょうせいネットの構築
・こうちぎょうせいネットの移行については、県と協議のうえ、構築すること。
・第２次の掲載記事やアップロードファイルが第３次でも参照及び更新できるよう移行すること。
・接続団体がコンテンツを制作、編集が可能な CMS 機能を提供すること。
・アクセスする接続団体ごとにアカウントを管理すること。
・県の組織改正に伴う課室の異動(登録、変更、削除)に対応すること。
・人事異動等の事由によるメールアカウント等の各種アカウントの運用(登録、変更、削除)を行うこと。
・接続団体の LGWAN 系セグメントからアクセスできる構成とすること。

エ　データファイルの安全な受渡対策
・インターネットへ送信する添付ファイルを対象とすること。
・添付ファイルをメール本文から分離し、メール側には残さない構成とすること。
・メールゲートウェイで添付ファイル分離後、送信メール本文に自動的にダウンロード URL を挿入すること。
・ファイルダウンロードにはパスワード認証を必須とすること。
・パスワード通知メールはファイル通知メールとは別のメールとして自動送信すること。
・ダウンロード URL には受託事業者がダウンロード回数制限を設定すること。
・また、登録後１週間を超えたファイルについては自動削除されること。

・添付ファイルは分離後、上記アのオンラインストレージに自動転送されること。
・外部 ASP/SaaS を利用するクラウド方式を利用する場合は、ISMAP クラウドサービスにおいて、基盤サービスとして登録されているだけでなく、サービスとしても登録されているクラウドサービスを利用すること。
・ユーザー数は構成団体の全職員が使用できることを想定すること。

オ　リモートメンテナンス

①リモートメンテナンス

・セキュリティクラウド内の仮想マシンに対して、外部からのリモート接続によりメンテナンスを行う機能を提供すること。

・リモートメンテンス専用のファイアウォールを、セキュリティクラウド運用監視／管理セグメントに構築し、リモートメンテナンス実施事業者ごとに、リモートメンテンス専用のファイアウォールから、対象のサーバに対して遠隔保守を行える環境を構築すること。
・リモートメンテナンスに係る責任範囲は、表２のとおりとする。

表２　リモートメンテナンスに係る責任範囲

主体	責任範囲・費用負担
・県 ・受託事業者	・リモートメンテナンス用の接続環境としてセキュリティクラウド内に配置する、リモートメンテナンス専用ファイアウォールまでの間を責任範囲とする。 ・リモートメンテナンス専用ファイアウォールは、県が設置する。
・接続団体 ・リモートメンテナンス実施事業者	・リモートメンテナンス実施事業者側から上記ファイアウォールまでの閉域網回線(情報ハイウェイ含む)及びリモートメンテナンス専用端末を責任範囲とする。 ・接続回線及びリモートメンテナンス専用端末は、リモートメンテナンス実施事業者が調達する。

・リモートメンテナンスを実施する場合の責任分界点及びセキュリティクラウドのセグメント概要は図３のとおり。

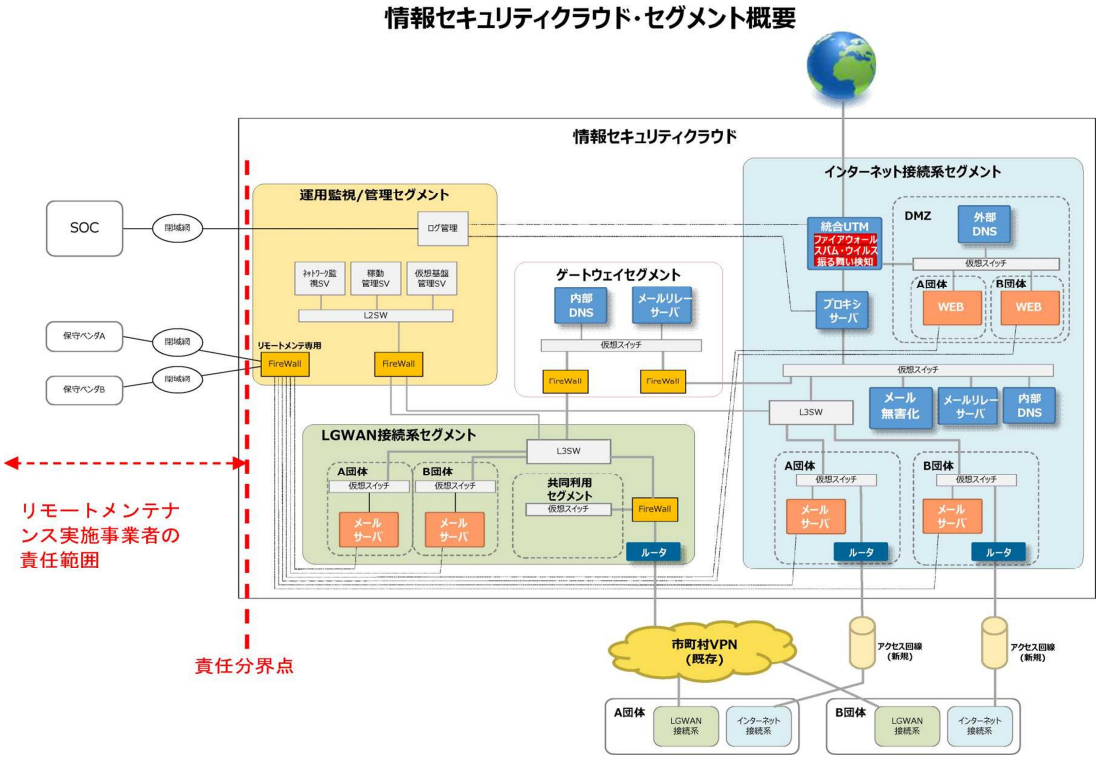

図３　セキュリティクラウド・セグメント概要

カ　個別オプションサービス

①仮想マシン等の提供

・第２次で提供している個別オプションサービスと同等のサービス(仮想マシン、Web サーバ、Web メールサーバ、メールサーバ等)を提供すること。(別紙５に記載)
・メーカーサポートを契約し、ハードウェア・ソフトウェアを包括的にサポートすること。
・共同基盤ではなくセキュリティクラウドの専用基盤上に構築、運用すること。
・第２次で個別オプションサービスとして稼働している仮想サーバを移行し、第３次での個別オプションサービスとして正常稼働を保証すること。
・仮想サーバに対して死活監視を行うこと。
・希望する接続団体については、仮想マシンの提供以外にもメールサーバの運用を行うこと。

②各種個別サービスの提供

・第２次で提供している以下の個別オプションサービスを継承すること。

A）Web サーバースターターパック
仮想マシンに RockyLinux と Web サーバをインストールするサービス

B）メールサーバースターターパック
仮想マシンに RockyLinux とメールサーバをインストールするサービス

C）メールサーバーサポートパック
スターターパックの内容に加えて、OS・ソフトウェアの設定、各種アカウントの登録・削除、ログ管理、セキュリティパッチ対応、問い合わせ対応を含めたサービス

D）グローバル IP アドレスの追加払い出し
グローバル IP アドレスを２個目以上希望する接続団体については、個別サービスとして提供すること

Ｅ）WAF 対象 FQDN 追加
WAF の対象 FQDN を２個以上希望する接続団体については、個別サービスとして提供すること
Ｆ）改ざん検知対象 URL 追加
改ざん検知の対象 URL を２個以上希望する接続団体については、個別サービスとして提供すること
(補足)
グローバル IP アドレス、WAF 対象 FQDN、改ざん検知対象 URL は、接続団体に各１個標準提供すること。

③接続団体個別アンチスパム
・インターネットからのメールセキュリティについて、接続団体個別のアンチスパムサーバを個別オプションサービスとして提供すること。
・オプションサービスを契約した接続団体ごとにブラックリスト／ホワイトリスト等のアンチスパムルールを管理できること。
・スパム判定されたメール原本をアンチスパムサーバに２週間以上保存すること。
・個別アンチスパム接続団体からの以下の依頼について、電話、FAX、電子メール、Web フォームによりヘルプデスクで受け付け、対応すること。
Ａ）ホワイトリスト登録
Ｂ）スパム判定された保存メールの原本再送
・保存されたスパム判定メールを無害化した上で、件名に特定の文字列を追記し、LGWAN 接続系のメールサーバに配送すること。なお、配送の際は送信元メールアドレス先頭に特定の文字列を付与し、接続団体から返信できないようにすること。

④アンチウイルス／スパム対策(LGWAN 系)
・希望する接続団体に対して、LGWAN との送受信メール等について、マルウェアの有無の検査を行い、マルウェアが検出された場合に隔離や削除等の処理を行うこと。
・LGWAN メールについて、迷惑メール・スパムメール等の判定を行い、レベルに応じて遮断、隔離やタグ付けなどの処理を行う機能を提供すること。
・パターンファイルは、自動更新により常に最新のものに更新すること。

⑤メール添付ファイル自動無害化
・業務利便性の観点からメール無害化処理とファイル無害化処理が連携し、メール添付ファイルを自動的に無害化し、メール宛先(LGWAN 接続系の転送先)へ送付する機能を有すること。
・自動的に無害化する/しないファイルの拡張子の設定が可能であること。なお、現行の無害化する/しないファイルの対象拡張子は別紙６のとおりである。
・接続団体ごとに添付ファイル削除又は自動無害化の選択が可能であること。

⑥メールアーカイブ
・対象とする送受信メールの原本（添付ファイルも含む）を受託事業者が５年程度保管できるサービスの提供ができること（オプションで期間を延長できること）。
・接続団体の管理者が、GUI を利用して、保存したメールデータを検索することができること。
・メール検索の結果、メール情報(本文、添付ファイル、件名、送信者、受信者、Cc、Envelop From、Envelop To、受信日時)を確認可能であること。その際に、文字セットを選択できること。また、メールが改ざんされていない旨のメッセージを確認可能であること。
・確認したメールについては、eml 形式にてダウンロード又は、元の配送先やメールアドレスを指定して配送することができ、件名にキーワードを挿入することも可能であること。その際に、送信日時(Date ヘッダ)を変更せずそのまま配送することが可能であることにくわえて、整合性エラー等が起こらないような提案とすること。

・原本メールサーバ・LGWAN メールサーバそれぞれ個別のメールアーカイブを可能とすること。その際、重複してアーカイブされることを避ける提案をすること。
・各接続団体のデータは論理的に分離され、他団体からのアクセスを遮断する構成とすること。なお、リソースの最適化のため、共通基盤上でのマルチテナント構成を許容するが、管理機能は団体ごとに独立して提供すること。
・契約終了後は受託事業者が保管データを電磁記録媒体等に収め、データの移行ができる形として提供すること。

⑦仮想ブラウザ
・αモデルを前提とし、LGWAN 接続系ネットワークからインターネットへ接続するための仮想ブラウザ機能を提供できること。
・接続団体ごとに仮想ブラウザの環境設定ができること。
・仮想ブラウザが Web 会議（カメラ・マイク使用）利用時においても、遅延なく操作可能なコンピュータリソース（仮想 CPU、メモリ、GPU アクセラレーション等）を動的に割り当てられること。
・LGWAN 接続系とのデータ転送を禁止とすること。
・インターネットからダウンロードしたファイルは仮想ブラウザ環境で無害化し、LGWAN 接続系に取り込めること。
・LGWAN 接続系プリンタでの印刷が可能であること。
・いつ、誰が、どのサイトを閲覧し、どのファイルをダウンロード／無害化したか操作ログを一元管理し、6ヶ月以上保存できること。
・ローカル・仮想ブラウザ間のテキスト(文字)のコピー&ペースト(片方向・双方向)が設定(権限)により接続団体単位で制御できること。
・ローカル・仮想ブラウザ間でファイル交換(片方向・双方向)が設定(権限)により接続団体単位で制御できること。
・仮想ブラウザで Web 会議システムが利用できること。
・物理端末の USB ポートに接続したスピーカー、マイク、カメラ等外部デバイスが利用できること。

⑧その他
・別紙５に記載のオプションサービス機能を提供すること。

２　非機能要件

（１）機器設置場所に関する要件

①設置場所
・セキュリティクラウドは、日本国内のデータセンターに設置・構築することとし、設置場所は受託事業者が提案するデータセンターとすること。
・ハウジング料金が発生する場合、契約終了日までのハウジング料金を運用経費に含めること。

②安全対策
・建築基準法の新耐震基準を満足した免震構造又は耐震構造であること。
・水没や浸水の恐れがないこと。
・消防法に基づき水損防止のためガス系消火設備及び火災感知設備を有すること。
・無停電電源装置等による電源トラブル対策がなされていること。
・入室を許可された者以外の立ち入りを禁じていること。
・生体認証等により、許可された者以外の入室を排除すること。
・入退室の記録がされていること。
・立入り検査が可能であること。
・メイン・バックアップ共に耐震性に優れ、新耐震基準に適合し、かつ ISMS 等の基準に準拠した震度６強に耐え得ることが確認できる施設であること。

・電源については本線・予備線の２系統受電、または異変電所からの受電が可能で、災害発生等による停電時にも、72 時間の連続運転が可能な設備を有していること。

（２）通信回線

①インターネット接続用回線

・物理的に異なる２系統の完全異ルートとし、各々10Gbps 以上の通信帯域を持つこと。このうち、セキュリティクラウドには、最低１Gbps 以上の帯域を保証すること。
・最低帯域の増速が可能であること。（追加料金を前提とする）
・512 個以上の IPv4 グローバル IP アドレスを提供すること。また、IP アドレスの必要数の追加に対応できること。
・IPv6 グローバル IP アドレスについても、必要数を提供すること。
・死活監視を行い、障害発生時には速やかに対応すること。また、監視装置についても、別監視装置を用いて、死活監視を行い、障害発生時には速やかに対応が可能な設計とすること。
・サービスに関する作業やトラフィックの推移状況、平均値については、ポータルサイトで情報提供し、接続団体が確認できる状況にすること。
・インターネット接続における冗長化方式は、複数の上位 AS との間で BGP による AS 間接続とすること。このときの経路制御及び負荷の分散については、当該 AS 間の経路情報の交換により、ロードバランスや代替経路、ボトルネックの解消などのトラフィック制御を行い実現すること。

②アクセス回線

・各接続団体からセキュリティクラウドへのアクセス回線については、一義的に情報ハイウェイの利用を想定している。情報ハイウェイの概要については、県デジタル政策課 HP(https://www.pref.kochi.lg.jp/doc/2019093000048/)及び高知県情報ハイウェイサービス HP（https://www.kochihw.jp/about/）で確認のうえ、利用規約及び技術要綱に準拠した構成とすること。提案書へ詳細な構成や接続方法などについて記載すること。（現在の最大帯域 10Gbps、平均トラフィック１Gbps）
・また、セキュリティクラウドへの接続口として、「セキュリティクラウド接続ルータ」を各接続団体に設置し、運用保守を行うこと。
・各接続団体からセキュリティクラウドまでの接続用回線は、現在の情報ハイウェイ利用状況も考慮し、情報ハイウェイのみでなく、その他の回線についても使用することができるようにすること。
・受託事業者が各接続団体に設置するアクセス回線用の通信機器より内側(庁内側)のネットワークの敷設や設定変更等は、各接続団体で行う。
・ISP の変更ができない接続団体については、接続団体→ISP→セキュリティクラウド→インターネットという経路で通信するための設定を行うこと。

（３）ネットワーク環境に関する要件

①委託業務範囲

・セキュリティクラウドの利用に必要となるネットワーク及び関連機器を準備し設定すること。
・ネットワークの準備に当たり、配管・施設工事等が発生する場合、当該作業は本業務の範囲に含めること。

②セキュリティクラウド運用基盤(基幹ネットワーク)

・インターネット通信、DMZ、LGWAN 通信(LGWAN メールリレー、LGWAN 接続ファイアウォールの監視等)の３つのネットワークに分割し、適切に運用すること。

③セキュリティクラウド接続用ネットワーク機器(各接続団体側)

・各接続団体からアクセス回線への出口は、接続団体ごとに基本的に各１ヵ所とし、セキュリティクラウド側と整合が取れるよう設計を行うこと。
・セキュリティクラウド接続ルータの適正な運用保守を行うこと。

④インターネット系ネットワークに関する要件
・各接続団体のインターネット系ネットワークの現行の IP アドレス体系を継承し、必要があれば再設計すること。

⑤LGWAN 系ネットワークに関する要件
・LGWAN に対して、データセンター内のネットワークを中継した IP リーチャビリティが発生しないよう、データセンター内の機器を構成すること。
・LGWAN との通信がインターネットからアクセス可能なセグメント上を経由しないこと。
・LGWAN のドメイン情報やルーティング情報がインターネット上に漏洩しないこと。
・各接続団体の LGWAN 系ネットワークを延伸し、現行の IP アドレス体系を継承すること。

⑥その他
・各接続団体のネットワーク保守や停止等によりセキュリティクラウドのサービス停止が発生しないネットワーク構成とすること。

（４）情報セキュリティ

①アクセス管理
・管理権限でアクセスする者の一人一人を識別し認証する機能を有すること。
・必要なアカウントを管理(登録、更新、権限設定、停止、削除等)し、システムにアクセスする者それぞれの役割に応じて、利用可能な機能、アクセス可能なデータ、実施できるデータの操作等を制限する機能を有すること。
・保守運用作業員のアクセス範囲を必要最低限のものとすること。
・保守運用作業員は閲覧権限によって、表示対象外データの存在自体を認識できないようにし、機密情報の秘匿性を保つこと。
・適切なシステムの操作記録(ログイン記録、操作ログ等)を取得すること。操作記録は、アカウント、アクセス年月日、アクセス時分、アクセス対象等の詳細な項目に細分化し、ログの取得を行うこと。
・ログは、損傷や紛失、消去から保護し最低１年間は保管すること。

②セキュリティインシデント防止対策
・各サーバ等への不正なアクセスを防ぐ仕組みを有していること。
・コンピュータウイルス等の不正なプログラムへの対策が取られていること。
・OS 等、システムを構成するソフトウェアについて、ソフトウェア開発元よりセキュリティパッチが提供された場合、速やかに評価・適用すること。
・セキュリティパッチの評価はテスト環境で行うこと。事前に県と協議を行い、作業スケジュールの調整を行うこと。
・適用作業実施後に動作確認を行い、結果を県に報告すること。
・再委託を行う場合は、本要件と同等のセキュリティ水準を維持することを再委託先と契約し、その管理状況を県に報告すること。

③セキュリティインシデント対応
・セキュリティインシデントが発生した場合、又はその恐れが高まった場合には、利用記録の解析及び結果の報告を行うこと。
・復旧作業終了後には、事故の原因・復旧に要した費用及び再発防止計画を文書化し、結果を県に報告すること。

④その他
・JIS Q 27001(ISO/IEC27001)及びプライバシーマークにおいて定められた情報管理基準を満たすために必要な教育、訓練を適宜実施すること。

・セキュリティクラウドの運用に関して、「高知県情報セキュリティポリシー」に従って実施することを基本とし、システムの機密性及び完全性を確保すること。
・その他セキュリティの向上に資する機能や取組みがある場合、県に提案すること。

（５）可用性

①可用性の確保

・セキュリティクラウドが提供するサービスの提供時間は、原則として 24 時間 365 日(閏年は 366 日)とする。
・セキュリティクラウドが提供するサービスついては、定期保守を除き 99.9%以上の稼働率を確保可能な可用性対策を講じること。
・可用性を確保するために、ネットワーク機器を含む設備及び機能、冗長化を行うこと。
・Web セキュリティ対策及び Web ブラウジングセキュリティ対策に関する可用性対策を講じること。
・メンテナンス等のため、サービスを利用できない時間が生じる場合には、１ヵ月前までに県に連絡し調整を行うことを原則とすること。
・予定したメンテナンス等日時に災害が発生又は発生が予想される場合は、直ちに中止又は延期が可能なこと。

②サービスの復旧

・セキュリティクラウド自体が攻撃を受けた場合の対応や、攻撃によりサービスが停止してしまった場合の回復に向けた対応について、県に提案し実施すること。

③事業継続計画（BCP）の策定と実施

・受託事業者は、本業務における BCP を策定し、契約後１ヶ月以内に県に提出し承認を得ること。
・BCP には、大規模災害、パンデミック、大規模なサイバー攻撃等のリスクを想定した対応手順、連絡網、及び代替手段を明記すること。
・受託事業者は、年１回以上の BCP 訓練（机上演習等）を実施し、その結果に基づき計画の見直しを適宜行うこと。
・災害等によるサービス停止時には、あらかじめ合意した目標復旧時間（RTO）に基づき、速やかな復旧に努めること。

（６）規模

・第２次の規模として示している別紙７を前提に、第３次の規模要件を作成し、県と協議のうえ合意した要件を満たすこと。

（７）拡張性・柔軟性

①変動要素への対応

・接続団体の追加、利用者数の増加、機器等の追加、回線増速等に対応できるよう、システムの拡張性を確保すること。
（特に利用者数は、接続団体数が多いことから、小幅な変動が多いと想定される）

②ネットワークモデル等への対応

・αモデルからその他のネットワークモデル等に移行する接続団体を許容するリソースの拡張性を確保し、将来的な増加に対応できるようにすること。
・ネットワークモデル移行団体に対して、新たな脅威へのセキュリティ対策や移行方法を具体的に提案すること。
・ネットワークモデル移行に伴い接続団体側で必要となるサービス等の調達については、本委託業務の範囲外とする。

第３章　テスト作業要件

１　テスト計画、実施及び評価

・受託事業者による動作確認テストについて、実施前にテスト実施計画書を提出し、県の承認を得ること。
・テスト実施計画書に従い、テストを実施すること。
・テストの実施に必要な関係者との調整を主体的に行うこと。
・摘出した不具合の管理と対処を確実に行うこと。
・テスト期間中の定例進捗会議において、テストの状況と見解を報告すること。
・テスト完了後、速やかにテスト結果及び品質の分析・評価を行い、報告書を県に提出すること。

２　テスト項目

①構成・設定確認

・設計書に記載されたネットワーク構成、ソフトウェア構成及び各種設定値に誤り(漏れ、論理矛盾を含む)が無いことを確認すること。
・設計書に記載されたネットワーク構成、ソフトウェア構成及び各種設定値が、実際の構成及び各種設定値と相違ないことを確認すること。

②疎通確認(主系／副系)

・各機器を接続したうえで、主系の疎通確認及び主系に障害が発生した際の従系による疎通確認を行うこと。

③機能確認(正常系／異常系)

・セキュリティクラウドの各機能別に、設定した内容で想定した動作(正常系／異常系)が行われることを確認すること。

④運用確認

・想定範囲内の同時アクセス数(外部／内部)及びトラフィック量において、問題なく利用できることを確認すること。
・想定を超える同時アクセス数(外部／内部)及びトラフィック量において、影響範囲と対処方法を確認すること。
・異常発生時の検知、対処及び復旧について想定どおり実施できることを確認すること。

第４章　移行作業要件

１　移行要件

①移行についての考え方

・各接続団体で行う庁内ネットワーク(LAN)の設定変更等について、各接続団体で必要となる移行作業の内容、作業実施主体等を明確にし、移行計画書に具体的に記述すること。

・第２次の移行対象は別紙８のとおり。

②移行計画の策定

・移行に係る作業は、移行計画書としてまとめ、県の承認を得たうえで実施すること。

・移行プロセスを明確にすることにより、接続団体や関係ネットワークベンダーとの認識齟齬を防ぎ、作業を円滑に進めること。

③データの保全

・移行期間中に送受信したメール等が消失しないよう考慮し計画を立てること。

④サービスやネットワークの停止

・稼働中のサービスやネットワークの停止を伴う作業を行う場合、閉庁日又は夜間での実施を考慮し、各接続団体と調整のうえで実施すること。

⑤その他

・多数の接続団体が接続するに当たり、考慮すべき事項やその対応について提案すること。

・各接続団体の関係ネットワークベンダーとの協議及び調整について、真摯に対応すること。

・第２次が提供するオプションサービスの仮想マシン及びデータ等の移行について、第２次の運用保守事業者及び接続団体並びに接続団体の関係ネットワークベンダー等と調整のうえで実施すること。

・移行の進捗状況及び移行結果について、適時県に報告すること。

２　各接続団体の移行支援

①構築・移行時の業務

・各接続団体へのヒアリング、移行作業に係る調整、問い合わせへの対応や個別打合せの実施等、各接続団体の移行作業を計画通りに進捗させるための支援を主体的に行うこと。

・セキュリティクラウドで提供する機能ごとに、各種コンテンツの移行、アカウント登録、データ移行など、各接続団体の状況に応じて、各種機器の設定変更や接続支援を行うこと。

・説明会の実施、各接続団体の関係ネットワークベンダーとの連携を行うこと。

・必要に応じて県及び各接続団体の庁舎で個別説明の機会を設けること。

・各接続団体のセキュリティ担当者や関係ネットワークベンダーに対して、仕様説明及び操作説明、移行支援を効果的に実施するための方法を提案すること。

②移行後・運用前の業務(機能検証期間の業務)

・各接続団体のセキュリティ担当者に対する説明会の実施及び接続団体の管理者向け説明会を実施すること。

第５章　運用サービス要件

１　運用設計

①SLA の策定

・委託業務期間における SLA は表３のとおりとする。
・受託事業者の瑕疵によりサービス稼働率を達成できなかった場合、本業務の月額料金を上限として、稼働率に応じた料金返還を実施する。

表３　SLA

大分類	小分類	サービスレベルの評価項目	サービス実施規定値等
可用性	サービス期間	点検・工事等による計画停止を除くサービス提供	24 時間 365 日(閏年は 366 日)
	計画停止予定通知	上位回線(ネットワーク)工事、施設点検等によりサービスの一時停止を行う場合の通知	停止日から３週間前までに連絡を行い、協議の上、作業の決定を行う。
	サービス稼働率	月間システム稼働率	99.9%以上
		稼働率(%)=(１－A／B)×100 A：サービス利用停止(※)時間(県承認済の停止作業時間は除く) B：計測期間(当該月)の日数 ※サービス利用停止とは、全接続団体がセキュリティクラウドを経由してインターネットへの接続ができない状態を指す。 ※情報ハイウェイの障害による停止時間は除外する。	料金返還率(月額利用料金を上限とする。) 99.9%未満：1%、　99.5%未満：3% 99.0%未満：10%、　97.0%未満：20% 95.0%未満：30%、　90.0%未満：100%
信頼性	稼働監視	各サービス提供機能について、サービスが正常に提供されていることを監視する。１秒おきに３回の機能確認を行い、３回とも正常が確認できない場合、障害発生と判断する。 監視方法：SNMP プロトコルによるレスポンス解析 監視内容：①HTTP 監視、②URL 監視、③DNS 監視、④SMTP 監視、⑤仮想サーバのリソース使用状況	監視間隔：５分 障害通知時間：平日 8:30～18:00 は 30 分以内、それ以外の時間帯は１時間以内(軽微な障害は、翌営業日の 9:00 まで)
	疎通監視	インターネット接続回線、セキュリティクラウド～各接続団体の接続回線について、１秒おきに３回の機能確認を行い、３回とも正常性が確認できない場合、障害発生と判断する。 監視方法：PING プロトコルによるレスポンス解析 監視内容：PING パケットの送達時間	監視間隔：５分 障害通知時間：平日 8:30～18:00 は 30 分以内、それ以外の時間帯は１時間以内(軽微な障害は、翌営業日の 9:00 まで)
	障害対応	各サービス提供機能の障害発生時は、原因究明に着手すると共に、影響範囲、対応方法、対応時間等を県に適時報告し、協議の上速やかに障害復旧作業を行う。障害復旧時、発生した障害への対応状況(障害内容、発生理由、影響範囲、対応経緯、実施作業、再発防止等)についての報告を行う。	着手時間：平日 8:30～18:00 は１時間以内、それ以外の時間帯は２時間以内 ※着手時点で県に一次報告を行う。 報告タイミング：対応後１営業日以内
ネットワーク	インターネット接続回線	インターネット接続環境を提供する。 ネットワーク機器及びネットワークトラフィック状況に関する各種統計の報告を行う。	回線速度：1Gbps(帯域保証型) 冗長回線及び複数 AS によるマルチホーム 報告タイミング：１回／月
セキュリティ	ファイアウォール	不正アクセスを検出するまでの時間 不正アクセスを検出後、通知までの時間	SOC による 24 時間 365 日(閏年は 366 日)監視 SOC 検知後１時間以内に NOC で情報を把握、顧客との取り決めに応じて通知
	ウイルスチェック	ウイルス情報の把握 パターンファイルの更新	SOC による 24 時間 365 日(閏年は 366 日)監視 SOC 検知後１時間以内に NOC でウイルス情報を把握 ベンダーリリース後６時間以内にパターンファイル更新
	セキュリティインシデント対応	最新セキュリティのセキュリティ情報を提供する間隔 セキュリティインシデント発生時の初動対応(緊急時)	SOC による 24 時間 365 日(閏年は 366 日)監視 SOC 検知後１時間以内に NOC で情報を把握、顧客との事前の取り決めによる連絡及び被害(加害)の拡散防止対策の実施

②運用設計書の作成及び掲載

以下の内容を運用設計書としてまとめ、県に納入するとともに、接続団体が閲覧できるようにポータルサイトに掲載すること。

・日次／月次／年次の業務運用サイクル(イベントスケジュール)
・接続団体と受託事業者との作業分担
・システム監視体制と監視項目
・バックアップ運用に関する情報(バックアップ対象及び方法、頻度、保存形式(全体／差分等)、世代数、保存先)
・システム出力ログに関する情報(種類、概要、出力タイミング、出力場所等)
・障害時対応(復旧・復元方法等)

2　運用要件

①サポート拠点の設置及びサポート体制の確立

・各接続団体の情報セキュリティ担当部署へのサポート及びセキュリティインシデント発生時の統括拠点を設置すること。
・運用要員を適切に配置すること。外部組織、協力会社、保守業者などが存在する場合、その関係、役割、作業分担、責任範囲、指揮系統を明確にすること。
・接続団体との窓口は一本化し、ワンストップで対応を実施すること。
・障害やセキュリティインシデント発生時の各接続団体との連絡体制を確立すること。
・緊急時における受託事業者内及び各接続団体への連絡体制図を整備し、あらかじめ関係者全員に配布すること。
・セキュリティインシデントが発生した場合、緊急度の程度により報告する手順・相手を明確にし、大規模災害などの障害時にも適切な対応をとること。
・障害発生時には、速やかに原因を特定し、適切に対応するとともに、県及び接続団体への報告、ポータルサイトへの掲載をすること。
・フィルタリングルール等各サーバ、ネットワーク機器の設定変更に迅速に対応できる体制を準備すること。

②運用手順書の整備

・運用に係る各作業については、手順書を作成し、それに基づいて作業を行うこと。
・運用手順書に基づいて作業を実施することで、運用の標準化・運用品質の向上を図ること。
・運用手順書は、PDCA により継続的に見直し・更新を行い、品質の向上を図ること。
・運用手順書は、ポータルサイトに掲載し、随時更新を行うこと
・運用フローを年１回以上見直すこと。

3　情報セキュリティの監視及びセキュリティインシデント対応

①SOC 監視体制

・SOC による監視は 24 時間 365 日(閏年は 366 日)の有人監視とする。セキュリティ運用基盤による迅速かつ高精度なセキュリティリスクの可視化に加え、専門のリスク分析官が詳細な解析を実施すること。
・セキュリティ機器が取得する PCAP も分析対象とし、各セキュリティ機器や SIEM が判断したリスクが高いイベントを追跡調査すること。
・10,000 人以上の規模の官公庁又は企業等において実績のあるセキュリティ監視・分析体制を敷くこと。
・セキュリティ監視業務を実施した経験を 10 年以上有していること。
・監視や分析によりセキュリティインシデントを検知した場合には、速やかに該当する接続団体に連絡するとともに、次項②に挙げる対応を行うこと。
・稼働状況、分析状況、セキュリティインシデントの検出状況及びセキュリティインシデントへの対応状況等について、月１回レポートを作成し、県に提出の上、全接続団体が確認できるようにポータルサイトに掲載すること。
・SOC で検知される新たなセキュリティインシデントについて、県に提示すること。
・新たなセキュリティインシデントの監視方法、検知実績、連絡体制、対応事例について、適宜報告を行うこと。
・監視に対する考え方、体制等について、分析対象となる機器及び通信、分析手法、セキュリティインシデント管理方法等を、運用開始前及び毎年度当初に県に説明すること。

②セキュリティインシデントへの対応

・セキュリティインシデントが発生した場合の対応について、深刻度に応じた対応フローや体制(役割分担)、各接続団体及び関係ネットワークベンダーとの連携方法等を整理し、運用開始前に県と合意すること。

・セキュリティインシデントを検知した場合、発生した接続団体を特定し、必要な初動対応を行うこと。
・セキュリティインシデント検知時には、専門分析官の提示する危険度のレベルと対応を表４のとおり定義し、定義に応じて必要な対応を実施すること。

表４　セキュリティインシデントのレベル定義と対応

レベル	定義	対応内容
Critical	攻撃成功が明白な場合	【重大なセキュリティインシデント】 電話・メールによる 緊急連絡
Serious	攻撃が成功した可能性が高い場合	
Medium	攻撃が発生しているが、影響がないと判断した場合	【軽微なセキュリティインシデント】 ドキュメントによる報告
Information	攻撃ではないが、注意が必要な場合	

・セキュリティインシデントの事案によっては、県の指示のもと該当する接続団体へ駆けつけ、必要となるログの収集、証拠証跡の確保を行うこと。
・セキュリティインシデントが発生した場合、情報漏えいを防ぐことを最優先として、ネットワーク接続の遮断等、必要な対応を行うこと。また、セキュリティインシデント情報の整理、事象の把握と調査を行い、被害の拡大防止を図ること。NOC においては、以下の対処を実施すること。

A)初動対応

	被害拡大防止と現状保存	事象の把握と調査	報告
実施内容	接続団体にヒアリングを行い、発生している事象やシステム構成を把握する。必要なログやデータの確保を依頼。 情報漏えいの可能性がある場合は、ネットワーク接続の遮断、システムや端末の状態保存、状態維持を依頼。	侵入手法や被疑端末の手掛かりをつかむため、その時点で入手できているログやデータから、不正アクセスの痕跡やマルウェア感染の状況を調査する。また、被害の拡大防止のための応急処置を検討する。	判明できた内容の報告と被害の拡大防止のための打ち手を、簡易報告書としてまとめて提出する。

・初動対応が完了した後、原因分析及び再発防止策案の検討を行い、接続団体による再発防止策の策定を支援すること。
・リスク許容度に応じて最適な復旧作業を提案し、実施すること。

B)調査・分析 C)改善提案

	調査・分析		改善提案
項目	原因・侵入手法の特定	影響範囲の明確化	改善提案
実施内容	攻撃・感染の痕跡の詳細分析や、必要に応じて、より高度な調査を行い、原因・侵入手法を特定する。	状況に応じて被疑端末だけでなく周辺端末の調査を行い、影響範囲を明確化する。	調査内容を総括して報告するとともに、再発防止の観点での実施事項をまとめる。
詳細	【調査手法の例】 ・アクセスログ解析／ネットワークログ解析／パケット解析／マルウェア解析		【提案例】 ・暫定的な構成変更／バージョンアップの推奨／プロファイリング／脆弱性診断

・セキュリティインシデントの発生を想定した訓練を年１回以上行うこと。(各接続団体へのメール及び FAX の一斉送信、ポータルサイトへの発生・対応状況の掲載等)

4 ヘルプデスク要件

①ヘルプデスクの設置

・各接続団体の情報セキュリティ担当部署の職員からの問い合わせ窓口としてヘルプデスクを設置すること(ポータルサイトの問い合わせも含む)。

②業務内容

・電話、FAX、電子メール、Web フォーム等を用意し、接続団体からの質問依頼・相談、障害、セキュリティインシデント等問い合わせに対応すること。
・接続団体からのオプションサービス機能の設定変更、各種アカウント(メールアカウント等)の設定変更等の各種手続の受付や、手続きの処理状況の照会に対応すること。
・技術的問い合わせ(各接続団体の情報セキュリティ担当職員からの問い合わせを含む)に対応できる体制をとること。
・ヘルプデスクへの問い合わせに対しては、可能な限りヘルプデスクから回答できる工夫をし、その場で回答できない場合には、運用部門等への照会を行うこと。
・対応履歴(ログ)の管理を行い、月次運用サービス実績報告書に記載すること。
・各種申請手続きについて Web フォーム等を用意し対応すること。
・セキュリティインシデントが発生した場合、SOC と連携し接続団体のセキュリティインシデント対応を行うこと。
・接続団体のインターネット系ネットワーク構成を入手し、構成情報を把握しておくこと。
・接続団体との接続で IP アドレス変換が行われている場合、接続団体側の IP アドレスとの変換情報を入手しておくこと。
・接続団体のシステム更新、システム変更に対し柔軟に対応すること。

・接続団体にてシステム更新、システム変更が行われた際、接続団体のネットワーク接続情報を最新化すること。

③対応条件

・ヘルプデスクは日本国内に設置し、日本語で対応可能であること。
・障害対応及びセキュリティインシデント対応については、24 時間 365 日(閏年は 366 日)対応可能なヘルプデスク窓口を用意すること。
・電話対応は、平日 8:30 から 17:15 まで受付し、応対すること。
・電子メール、FAX、Web フォーム等は 24 時間受付を行い、受付時間外に受信した問い合わせへの回答は、翌開設日に対応すること。
・受付電話は２回線以上とすること。
・問い合わせ者やその内容等の漏えい・紛失を防ぐ対策を行うこと。

④運用体制の確保

・運用責任者を設置し、問題への対応、指示などを適切に行える体制を整えること。
・セキュリティインシデント検知及び障害発生時の問い合わせに対応できる体制をとること。
・応対者については必要な教育を実施し、円滑なヘルプデスク対応を実現すること。
・応対者は、電話対応時間中は回線数プラス１名以上を確保し、運用に支障を生じさせないこと。

５　運用サポート(日常運用業務)

①運用に係る障害対応要件

・障害対応は 24 時間 365 日(閏年は 366 日)対応とする。
・障害発生から初期対応を開始するまでの時間を、概ね 30 分以内とすること。ただし、大規模災害発生時はこの限りではない。なお、初期対応とは、障害発生箇所・原因の確認作業への着手、県及び接続団体等の関係者への連絡等を指す。
・重要障害の発生を想定した訓練を年１回以上行うこと。(各接続団体へのメール及び FAX の一斉送信、ポータルサイトへの発生・対応状況の掲載等)
・不具合の修正、ソフトウェアのバージョンアップ、脆弱性への対応等を行い、ソフトウェアを適切に維持・管理すること。

②運用環境保全

・データバックアップ、リストア
・稼働監視
・性能・構成管理
・ログ管理
・バージョンアップ、パッチによる影響等の情報提供
・バージョンアップ、パッチインストール作業
・障害対応及び障害後是正措置・予防措置
・運用マニュアル等ドキュメントの改訂

③ドキュメント管理

・各種納入成果物について、運用期間中に内容の変更が生じた場合には、随時改訂を行い、更新履歴を付して県に提出するとともに、ポータルサイトへの掲載内容も更新すること。

④接続団体サポート

・ヘルプデスク業務
・各接続団体の状況や要望に応じて、各種設定変更や接続支援を行うこと。
・ユーザーアカウントの登録削除を行うこと。
・セキュリティクラウド内で使用するアカウントについては、毎年度更新することとし、更新後のアカウントについては、受託事業者から接続団体に通知すること。
・セキュリティクラウドへ新たに参加する団体から問い合わせがあった場合には、技術的な支援を行うこと。

⑤連絡会議

・次の要件に従い、連絡会議を定期的に開催し、運用状況を県及び必要に応じて接続団体に報告すること。
  - 原則として対面にて毎月１回開催すること。
  - 連絡会議終了後、速やかに、当該会議の議事内容について議事録を作成し、県及び接続団体に提出すること。

⑥運用スケジュール表及び運用実績報告書の提出等

・年間の運用スケジュール表を県及び接続団体に提出し、事前に運用スケジュール調整すること。
・運用実績報告書を県及び接続団体に提出し、その内容について詳細に説明すること。またポータルサイトでも情報提供すること。なお、運用実績報告書の記載内容は、次のとおりとする。
  Ａ）作業項目ごとの実施状況(作業日時、作業者、作業内容、作業場所等)
  Ｂ）ヘルプデスクへの質問及び回答内容(日時、質問者、内容、受付者、回答者、回答内容等)
  Ｃ）不正アクセスレポート(攻撃種類、件数等)
  Ｄ）その他必要事項(課題管理等)
  Ｅ）改善提案等

⑦説明会・会議等

・必要に応じて、接続団体向けに説明会を実施すること。
・県が主催するセキュリティクラウドに関する会議において、技術的な説明が必要な場合は、受託事業者が県の要望に応じて説明を行うものとする

第６章　構築作業体制及び構築方法

１　作業体制及び構築方法

①作業体制

・受託事業者は、業務を円滑に進めるために十分な体制を取ること。
・契約締結後、速やかにプロジェクト計画書(体制図含む)を県に提出すること。
・プロジェクト責任者及びプロジェクトを管理・主導する者は、事前に県が承認した場合を除き、契約日からセキュリティクラウドの運用開始日までの期間中、同一の人物とすること。
・県は、プロジェクト責任者等の業務遂行が不適切であると認める場合、受託事業者に対して当該者の交代を請求できるものとする。この場合、受託事業者は速やかに適切な後任者を選定し、県の承認を得るものとする。交代にあたっては、十分な引き継ぎ期間を設け、プロジェクトの品質及び納期に影響を与えないよう受託事業者の責任において万全の措置を講じること。

②プロジェクト計画

・契約後速やかにプロジェクト計画書を作成し、県の承認を得ること。
・プロジェクト計画書に変更の必要が生じた場合、都度県に更新版を提出し、承認を得ること。
・プロジェクト計画書に記述するべき主たる項目を、以下に示す。なお、C）体制図には、各要員の保有する技術的な資格及び今回の構築で利用する技術を用いた業務の経験を記載すること。また、D）スケジュールについては、合理的なスケジュールを作成すること。構築を効率的に進める手法があれば、併せて提案すること。
  A）プロジェクトの目的
  B）プロジェクト管理方針
  C）体制図
  D）スケジュール
  E）進捗管理計画
  F）コミュニケーション管理計画
  G）品質管理計画
  H）リスク管理計画(課題管理含む)
  Ⅰ）WBS

③プロジェクト管理

・プロジェクト計画に従い、主体的にプロジェクト管理を実施すること。
・進捗状況の確認、各種打合せ、リスクや問題の共有のため、構築期間中、月に２回程度進捗会議を行うこと。
・進捗の遅れ等、プロジェクトに問題が生じた場合には、頻度を上げて開催する等、状況に応じ柔軟に対応すること。
・進捗会議後には速やかに議事録を作成し、県の承認を得ること。
・品質低下や納期遅延に繋がる課題の予兆を検知し、防止に努めること。
・課題や問題点の発生時には、主体的に対策を検討し、県と協議のうえ対応を行うこと。
・運用に際しての残課題(申送り事項や制限事項)がある場合は、文書にて県に報告し、承認を得ること。

第７章　契約条件等

１　受託事業者の要件

①情報セキュリティを確保するための体制の整備

・本業務を実施する組織・部署において、本業務の実施を適用範囲に含んだ ISMS(情報セキュリティ管理システム)について ISO/IEC 27000 ファミリー規格の認証を取得していること。

・プライバシーマーク認定証、又はこれと同等の個人情報保護マネジメントシステムを確立していること。

②事業実績

・元請として、国、都道府県、市町村又は特別区の庁内ネットワークを構築・運用した実績を有すること。

・元請として、国、都道府県、市町村又は特別区において、LGWAN ネットワークを構築・運用した実績又は LGWAN を利用して通信を行うシステムを構築・運用した実績を有すること。

２　契約期間及び契約方法

①契約期間

・セキュリティクラウド構築・移行については、契約締結の日から令和９年３月 31 日までとする。

・セキュリティクラウド運用保守については、令和９年４月１日から令和 14 年３月 31 日までとする。

②契約主体

・構築及び運用保守に関する契約は、県と行うこと。

③オプションサービス契約

・セキュリティクラウドのオプションサービスに関しては、各接続団体との契約を行うこととし、支払方法や課金単位(月額単価、クライアント単価、アカウント単価など)に関する条件を、オプションサービス価格表(兼オプションサービス申込書)に記述すること。

３　委託業務終了時の対応

①各種情報の提供

・接続団体がシステムに登録したデータ(初期移行により登録したデータを含む)やログデータ、仮想 OS のイメージデータ等各種情報資産を、電磁記録媒体等に納め、接続団体に提出すること。

・メールデータ等の移行についても提案すること。

②プロジェクト管理

・業務終了及び第４次高知県情報セキュリティクラウドへの移行支援にかかるプロジェクト管理を行うこと。

③データ消去

・本業務の契約の中で、接続団体及び受託事業者がシステムに登録した全てのデータを、不可逆的な消去レベルの高い規格・手法にて消去し、データ消去終了後にはデータ消去証明書を発行すること。

4　第４次高知県情報セキュリティクラウドへの移行支援

①移行支援

・第４次においても業務を滞りなく継続するため、第３次で使用している、移行に必要な各種情報資産を提供すること。
・第４次の移行に必要な情報の開示等、積極的に協力すること。
・移行支援内容について、提案すること。

②移行対象資産

・各接続団体がシステムに登録した情報のすべて(初期登録データを含む)。
・移行に必要なシステムの設定情報。
・移行に必要なネットワークの設定情報等。
・移行対象資産の情報提供は、本業務の範囲内とする。
・移行対象資産の情報提供期日は、別途協議のうえ定める。